

Please amend the present application as follows:

Claims

The following is a copy of Applicant's claims that identifies language being added with underlining ("____") and language being deleted with strikethrough ("~~_____~~") or brackets ("[[]]"), as is applicable:

1. (Currently amended) A method for providing recipient-end security for transmitted data, the method comprising:

scanning a hard copy document with a data transmitting device to generate scanned data;

configuring the scanned data on the data transmitting device so as to require recipient-end security such that machine-specific security data that identifies a data receiving device to which the scanned data will be transmitted is verified prior to enabling access to the transmitted data;

transmitting the scanned data from the data transmitting device to ~~an intended recipient~~ the data receiving device;

determining on the data receiving device if the transmitted data may be accessed ~~at the recipient end~~ by verifying the machine-specific security data; and

denying access to the transmitted data if it is determined that the transmitted data may not be accessed.

2. (Canceled)

3. (Currently amended) The method of claim 1, wherein configuring the scanned data further comprises configuring the scanned data such that recipient-specific security information must be provided by a recipient of the transmitted data prior to accessing the transmitted data.

4. (Currently amended) The method of claim 3, wherein configuring the scanned data comprises configuring the scanned data such that the recipient must provide ~~at least one of a recipient password and~~ recipient biometric information to access the transmitted data.

5. (Canceled)

6. (Currently amended) The method of claim ~~5~~ 1, wherein configuring the scanned data comprises configuring the scanned data such that at least one of a ~~global logon password~~, an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data~~ is verified.

7. (Original) The method of claim 1, wherein transmitting the scanned data comprises faxing the scanned data.

8. (Original) The method of claim 1, wherein transmitting the scanned data comprises digitally sending the scanned data as an email attachment.

9. (Currently amended) The method of claim 1, wherein determining if the transmitted data may be accessed comprises verifying ~~required recipient-specific security information provided by a recipient that intends to access the transmitted data~~ recipient biometric information.

10-11. (Canceled)

12. (Currently amended) The method of claim ~~44~~ 1, wherein ~~verifying required machine-specific security information~~ determining if the transmitted data may be accessed comprises verifying at least one of a ~~global login password~~, an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data is verified~~.

13. (Currently amended) The method of claim 1, further comprising, ~~providing access to the transmitted data~~ if it is determined that the transmitted data may be accessed, ~~at the recipient end~~ printing out the transmitted data or opening an email attachment that comprises the transmitted data.

14. (Canceled)

15. (Currently amended) A system for providing recipient-end security for transmitted data, the system comprising:

means for configuring scanned data representative of a hard copy document so as to require ~~recipient-end security at a recipient end of a transmission path~~ verification of machine-specific security data that identifies a data receiving device to which the scanned data will be transmitted;

means for determining if the scanned data may be accessed at the recipient end ~~by requiring at least one of recipient-specific security information and~~ that verifies the machine-specific security information; and

means for denying access to the transmitted data if it is determined that the required machine-specific security information is not correct.

16. (Currently amended) The system of claim 15, wherein the means for configuring further comprise means for configuring the scanned data such that ~~at least one of a recipient password and recipient biometric information is~~ also required to access the scanned data.

17. (Currently amended) The system of claim 15, wherein the means for configuring comprise means for configuring the scanned data such that at least one of a ~~global login password, an Internet protocol (IP) address~~ [[,]] and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data is required to access the scanned data~~ is verified.

18. (Currently amended) The system of claim 15, wherein the means for determining comprise means for verifying ~~at least one of a recipient password and~~ recipient biometric information.

19. (Currently amended) The system of claim 15, wherein the means for ~~verifying~~ determining comprise means for verifying at least one of ~~a global logon password,~~ an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data is verified.~~

20. (Currently amended) A system stored on a computer-readable medium, the system comprising:

sender-end logic adapted to execute on a data transmitting device, the sender-end logic being configured to configure data scanned by the data transmitting device so as to require ~~recipient-end security at a recipient end of a transmission path~~ verification of machine-specific security data that identifies a data receiving device to which the scanned data will be transmitted; and

recipient-end logic adapted to execute on a data receiving device, the recipient-end logic being configured to ~~determine if the scanned data may be accessed at the recipient end by verifying~~ verify ~~at least one of recipient specific security information provided by a recipient of the scanned data and~~ the machine-specific security information of the data receiving device.

21. (Currently amended) The system of claim 20, wherein the sender-end logic is further configured to require ~~at least one of a recipient password and~~ recipient biometric information of the recipient prior to access of the scanned data.

22. (Currently amended) The system of claim 20, wherein the sender-end logic is configured to require verify at least one of a ~~global login password~~, an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data is verified before a recipient access the scanned data.~~

23. (Currently amended) The system of claim 20, wherein the recipient-end logic is configured to verify ~~at least one of a recipient password and~~ recipient biometric information prior to providing access to the scanned data.

24. (Currently amended) The system of claim 20, wherein the recipient-end logic is configured to verify at least one of a ~~global login password~~, an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of a the data receiving device ~~that received the transmitted data prior to providing access to the scanned data.~~

25. (Currently amended) A sender-end security manager stored on a computer-readable medium of a data transmitting device, the manager comprising:

logic configured to identify a type of recipient-end security to provide for ~~[[a]]~~ data scanned by the data transmitting device; and

~~logic configured to configure the scanned data to facilitate the identified type of recipient-end security~~ add security information to the scanned data that is to be used as a reference against at least one of recipient-specific security information that identifies a recipient who wishes to access the scanned data and machine-specific security information that identifies a data receiving device to which the scanned data will be transmitted.

26. (Canceled)

27. (Currently amended) ~~The manager of claim 25, wherein the logic configured to configure the scanned data comprises logic configured to~~ A sender-end security manager stored on a computer-readable medium of a data transmitting device, the manager comprising:

logic configured to identify a type of recipient-end security to provide for data scanned by the data transmitting device; and

logic configured to add an executable that is configured to verify at least one of recipient-specific security information entered by a recipient of the scanned data and machine-specific security information of a data receiving device that received the scanned data.

28. (Canceled)

29. (Currently amended) A recipient-end security manager stored on a computer-readable medium of a data receiving device, the manager comprising:

logic configured to identify a type of recipient-end security that is required to access data that has been received by the data receiving device; and

logic configured to verify ~~recipient-end security information~~ recipient biometric information prior to enabling access to the data.

30. (Canceled)

31. (Currently amended) ~~The manager of claim 29, wherein the logic configured to verify recipient-end security information comprises~~ A recipient-end security manager stored on a computer-readable medium of a data receiving device, the manager comprising:

logic configured to identify a type of recipient-end security that is required to access data that has been received by the data receiving device; and

logic configured to verify at least one of a global logon password, an Internet protocol (IP) address~~[[,]]~~ and a media access control (MAC) address of the data receiving device.